

*Commenced Publication in 1973*

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

## Editorial Board

David Hutchison

*Lancaster University, Lancaster, UK*

Takeo Kanade

*Carnegie Mellon University, Pittsburgh, PA, USA*

Josef Kittler

*University of Surrey, Guildford, UK*

Jon M. Kleinberg

*Cornell University, Ithaca, NY, USA*

Friedemann Mattern

*ETH Zurich, Zurich, Switzerland*

John C. Mitchell

*Stanford University, Stanford, CA, USA*

Moni Naor

*Weizmann Institute of Science, Rehovot, Israel*

C. Pandu Rangan

*Indian Institute of Technology, Madras, India*

Bernhard Steffen

*TU Dortmund University, Dortmund, Germany*

Demetri Terzopoulos

*University of California, Los Angeles, CA, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

Gerhard Weikum

*Max Planck Institute for Informatics, Saarbrücken, Germany*

More information about this series at <http://www.springer.com/series/7410>

Joaquin Garcia-Alfaro · Guillermo Navarro-Arribas  
Hannes Hartenstein · Jordi Herrera-Joancomartí (Eds.)

# Data Privacy Management, Cryptocurrencies and Blockchain Technology

ESORICS 2017 International Workshops, DPM 2017  
and CBT 2017, Oslo, Norway, September 14–15, 2017  
Proceedings

*Editors*

Joaquin Garcia-Alfaro  
Télécom SudParis  
Evry  
France

Guillermo Navarro-Arribas  
Department of Information  
and Communications Engineering  
Autonomous University of Barcelona  
Bellaterra  
Spain

Hannes Hartenstein  
Karlsruhe Institute of Technology  
Karlsruhe  
Germany

Jordi Herrera-Joancomarti  
Autonomous University of Barcelona  
Bellaterra  
Spain

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-319-67815-3              ISBN 978-3-319-67816-0 (eBook)  
DOI 10.1007/978-3-319-67816-0

Library of Congress Control Number: 2017953409

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer International Publishing AG 2017

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Printed on acid-free paper

This Springer imprint is published by Springer Nature  
The registered company is Springer International Publishing AG  
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

## Foreword from the DPM 2017 Program Chairs

This volume contains the proceedings of the 12th Data Privacy Management International Workshop (DPM 2017), held in Oslo, Norway, during September 14–15, 2017, in conjunction with the 22nd European Symposium on Research in Computer Security (ESORICS) 2017. The DPM series started in 2005 when the first workshop took place in Tokyo (Japan). Since then, the event has been held in different venues: Atlanta, USA (2006); Istanbul, Turkey (2007); Saint Malo, France (2009); Athens, Greece (2010); Leuven, Belgium (2011); Pisa, Italy (2012); Egham, UK (2013); Wroclaw, Poland (2014); Vienna, Austria (2015); and Crete, Greece (2016).

The aim of DPM is to promote and stimulate the international collaboration and research exchange in areas related to the management of privacy-sensitive information. This is a very critical and important issue for organizations and end-users. It poses several challenging problems, such as translation of high-level business goals into system-level privacy policies, administration of sensitive identifiers, data integration and privacy engineering, among others.

For this workshop edition we received 51 submission, and each one was evaluated on the basis of significance, novelty, and technical quality. The Program Committee, formed by 41 members, performed an excellent task and with the help of an additional 18 referees all submissions went through a careful review process (three or more reviews per submission). In the end, 16 full papers were accepted for presentation at the event. In addition, the program was completed with a keynote talk given by Vicenç Torra (University of Skövde, Sweden) on integral privacy (privacy models and disclosure risk).

We would like to thank everyone who helped organize the event, including all the members of the Organizing Committee of both ESORICS and DPM 2017.

Our gratitude goes also to Pierangela Samarati, Steering Committee Chair of the ESORICS Symposium, for all her arrangements to make possible the satellite events, and Socratis Katsikas, Workshops Chair of ESORICS 2017. Last but by no means least, we thank all the DPM 2017 Program Committee members, additional reviewers, all the authors who submitted papers, and all the workshop attendees.

Finally, we want to acknowledge the support received from the sponsors of the workshop: Institut Mines-Telecom (Telecom SudParis), CNRS Samovar UMR 5157 (R3S team), Universitat Autònoma de Barcelona, UNESCO Chair in Data Privacy, Universitat Rovira i Virgili, and project TIN2014-55243-P from the Spanish MINECO.

August 2017

Joaquin Garcia-Alfaro  
Guillermo Navarro-Arribas

# Organization

## 12th International Workshop on Data Privacy Management — DPM 2017

### Program Committee Chairs

Joaquin Garcia-Alfaro      Telecom SudParis, Paris-Saclay University, France  
Guillermo Navarro-Arribas      Universitat Autònoma de Barcelona, Spain

### Program Committee

Günes Acar      KU Leuven, Belgium  
Jordi Casas-Roma      Universitat Oberta de Catalunya, Spain  
Jordi Castella-Roca      Universitat Rovira i Virgili, Spain  
Frederic Cuppens      Telecom Bretagne, France  
Nora Cuppens-Bouahia      Telecom Bretagne, France  
Josep Domingo-Ferrer      Universitat Rovira i Virgili, Spain  
Christian Duncan      Quinnipiac University, USA  
Sara Foresti      Università degli Studi di Milano, Italy  
Sebastien Gambs      Université du Québec à Montréal, Canada  
Paolo Gasti      New York Institute of Technology, USA  
Marit Hansen      Unabhängiges Landeszentrum für Datenschutz,  
Germany  
Jordi Herrera-Joancomarti      Universitat Autònoma de Barcelona, Spain  
Masahiro Inuiguchi      Osaka University, Japan  
Marc Juarez      KU Leuven, Belgium  
Florian Kammüller      Middlesex University London, UK  
Hiroaki Kikuchi      Meiji University, Japan  
Evangelos Kranakis      Carleton University, Canada  
Maryline Laurent      Telecom SudParis, Paris-Saclay University, France  
Giovanni Livraga      Università degli Studi di Milano, Italy  
Javier Lopez      University of Malaga, Spain  
Brad Malin      Vanderbilt University, USA  
Chris Mitchell      Royal Holloway, UK  
Tarik Moataz      Brown University, USA  
Refik Molva      EURECOM, France  
Anna Monreale      University of Pisa, Italy  
Jordi Nin      BBVA Data & Analytics, Spain

Melek Önen	EURECOM, France
Cristina Pérez-Solà	Universitat Autònoma de Barcelona, Spain
Silvio Ranise	FBK, Security and Trust Unit, Trento, Italy
Kai Rannenberg	Goethe University, Germany
Yves Roudier	Université de Nice, France
Pierangela Samarati	Università degli Studi di Milano, Italy
David Sanchez	Universitat Rovira i Virgili, Spain
Claudio Soriente	Telefonica Research and Development, Spain
Matthias Templ	Vienna University of Technology, Austria
Vicenç Torra	University of Skövde, Sweden
Yasuyuki Tsukada	Kanto Gakuin University, Japan
Alexandre Viejo	Universitat Rovira i Virgili, Spain
Jens Weber	University of Victoria, Canada
Lena Wiese	University of Göttingen, Germany
Nicola Zannone	Eindhoven University of Technology, The Netherlands

### **Steering Committee**

Josep Domingo-Ferrer	Universitat Rovira i Virgili, Spain
Joaquin Garcia-Alfaro	Telecom SudParis, Paris-Saclay University, France
Guillermo Navarro-Arribas	Universitat Autònoma de Barcelona, Spain
Vicenç Torra	University of Skövde, Sweden

### **Additional Reviewers**

Carles Anglès-Tafalla	Wanpeng Li
Monir Azraoui	Fatma Al Maqbali
Sergi Delgado-Segura	Ana Nieto
Gerardo Fernandez	Jose A. Onieva
José Maria de Fuentes	Alfredo Rial
Akos Grosz	Sara Ricci
Paolo Guarda	Ruben Rios
Daniel Homann	Jordi Ribes-González
Ibrahim Lazrig	Hari Siswantoro

## Foreword from CBT 2017 Program Chairs

This volume contains the proceedings of the First International Workshop on Cryptocurrencies and Blockchain Technology (CBT 2017) held in Oslo, Norway, on September 14, 2017, in conjunction with the 22nd European Symposium on Research in Computer Security (ESORICS) 2017.

Since the appearance of Bitcoin in 2009, a plethora of new cryptocurrencies and other blockchain-based systems have been proposed and deployed. While some of them are slightly different copies of Bitcoin, others propose interesting improvements or new usages of the underlying blockchain technology. Owing to their construction as blockchain-based systems, security and dependability aspects need to be rigorously designed and analyzed. The goal of the CBT workshop is to provide a forum for researchers in this area to carefully analyze current systems and propose new ones in order to create a scientific background for the solid development of new cryptocurrencies and blockchain technology systems.

In response to the call for papers, we received 27 submissions that were carefully reviewed by the Program Committee comprising 15 members and by additional reviewers. Each submission received at least three reviews. The Program Committee selected six papers as full papers (resulting in an acceptance rate of about 22%) and four short papers for presentation at the workshop. The selected papers cover aspects of identity management, smart contracts, soft- and hardforks, proof-of-works and proof-of-stake as well as on network layer aspects and the application of blockchain technology for secure concert/event ticketing.

Furthermore, the workshop was enhanced by the keynote offered by Prof. Roger Wattenhofer, a talk that was made possible thanks to the sponsorship of Blockchain Inc.

We would like to thank all the authors who submitted papers to CBT 2017 and the Program Committee and the additional reviewers who worked hard to review the submissions and discussed the final program. We would also like to thank the ESORICS workshop chair Sokratis Katsikas and his team as well as the ESORICS organizers for putting faith in us and in the topic of cryptocurrencies and blockchain technology.

We hope that you find the proceedings of CBT 2017 interesting and inspiring and that there will be follow-ups of the CBT workshop in the coming years.

Jordi Herrera-Joancomartí  
Hannes Hartenstein



# First International Workshop on Cryptocurrencies and Blockchain Technology CBT 2017

## Program Committee Chairs

Hannes Hartenstein                      Karlsruher Institut für Technologie, Germany  
Jordi Herrera-Joancomartí              Universitat Autònoma de Barcelona, Spain

## Program Committee

Rainer Böhme                              Universität Innsbruck, Austria  
Jeremy Clark                                Concordia University, Canada  
Christian Decker                            Blockstream, USA  
Joaquin Garcia-Alfaro                    Telecom SudParis, Paris-Saclay University, France  
Arthur Gervais                              ETH, Switzerland  
Man Ho Au                                  The Hong Kong Polytechnic University, SAR China  
Ghassan Karame                            NEC Research, Germany  
Stefan Katzenbeisser                    Technische Universität Darmstadt, Germany  
Patrick McCorry                            UCL, UK  
Shin'ichiro Matsuo                        BSafe.network and Keio University, Japan  
Guillermo Navarro-Arribas              Universitat Autònoma de Barcelona, Spain  
Mariusz Nowostawski                    NTNU, Norway  
Cristina Pérez-Solà                        Universitat Autònoma de Barcelona, Spain  
Roger Wattenhofer                        ETH, Switzerland

## Steering Committee

Rainer Böhme                              Universität Innsbruck, Austria  
Joaquin Garcia-Alfaro                    Telecom SudParis, Paris-Saclay University, France  
Hannes Hartenstein                        Karlsruher Institut für Technologie, Germany  
Jordi Herrera-Joancomartí              Universitat Autònoma de Barcelona, Spain

## Additional Reviewers

Svetlana Abramova                        Shinichi Miyazawa                        Paulina Pesch  
Sergi Delgado-Segura                    Ken Naganuma                              Kazue Sako  
Michael Fröwis                              Till Neudecker                              Oliver Stengele

# Contents

## Privacy, Logics, and Computational Models

A Proof Calculus for Attack Trees in Isabelle . . . . .	3
<i>Florian Kammüller</i>	
Confidentiality of Interactions in Concurrent Object-Oriented Systems . . . . .	19
<i>Olaf Owe and Toktam Ramezanifarkhani</i>	
Using Oblivious RAM in Genomic Studies . . . . .	35
<i>Nikolaos P. Karvelas, Andreas Peter, and Stefan Katzenbeisser</i>	

## Privacy and Encrypted Search

Towards Efficient and Secure Encrypted Databases: Extending Message-Locked Encryption in Three-Party Model . . . . .	55
<i>Yuuji Furuta, Naoto Yanai, Masashi Karasaki, Katsuhiko Eguchi, Yasunori Ishihara, and Toru Fujiwara</i>	
Searchable Encrypted Relational Databases: Risks and Countermeasures . . . . .	70
<i>Mohamed Ahmed Abdelraheem, Tobias Andersson, and Christian Gehrman</i>	
Private Verification of Access on Medical Data: An Initial Study . . . . .	86
<i>Thais Bardini Idalino, Dayana Spagnuolo, and Jean Everson Martina</i>	

## Data Privacy, Data Mining, and Applications

Default Privacy Setting Prediction by Grouping User's Attributes and Settings Preferences. . . . .	107
<i>Toru Nakamura, Welderufael B. Tesfay, Shinsaku Kiyomoto, and Jetzabel Serna</i>	
$\delta$ -privacy: Bounding Privacy Leaks in Privacy Preserving Data Mining . . . . .	124
<i>Zhizhou Li and Ten H. Lai</i>	
Threshold Single Password Authentication . . . . .	143
<i>Devriş İşler and Alptekin Küpçü</i>	
Towards a Toolkit for Utility and Privacy-Preserving Transformation of Semi-structured Data Using Data Pseudonymization . . . . .	163
<i>Saffija Kasem-Madani, Michael Meier, and Martin Wehner</i>	

**User Privacy**

Privacy Dashcam – Towards Lawful Use of Dashcams  
Through Enforcement of External Anonymization . . . . . 183  
*Paul Wagner, Pascal Birnstill, Erik Krempel, Sebastian Brethauer,  
and Jürgen Beyerer*

DLoc: Distributed Auditing for Data Location Compliance in Cloud . . . . . 202  
*Mojtaba Eskandari, Bruno Crispo, and Anderson Santana de Oliveira*

Inonymous: Anonymous Invitation-Based System . . . . . 219  
*Sanaz Taheri Boshrooyeh and Alptekin Küpçü*

**Applied Cryptography and Privacy**

PCS, A Privacy-Preserving Certification Scheme. . . . . 239  
*Nesrine Kaaniche, Maryline Laurent, Pierre-Olivier Rocher,  
Christophe Kiennert, and Joaquin Garcia-Alfaro*

Order-Preserving Encryption Using Approximate Integer  
Common Divisors . . . . . 257  
*James Dyer, Martin Dyer, and Jie Xu*

Privacy-Preserving Deterministic Automata Evaluation  
with Encrypted Data Blocks . . . . . 275  
*Giovanni Di Crescenzo, Brian Coan, and Jonathan Kirsch*

**Consensus and Smart Contracts**

Securing Proof-of-Stake Blockchain Protocols. . . . . 297  
*Wenting Li, Sébastien Andreina, Jens-Matthias Bohli,  
and Ghassan Karame*

Merged Mining: Curse or Cure? . . . . . 316  
*Aljosha Judmayer, Alexei Zamyatin, Nicholas Stifter,  
Artemios G. Voyiatzis, and Edgar Weippl*

Atomically Trading with Roger: Gambling on the Success of a Hardfork . . . . 334  
*Patrick McCorry, Ethan Heilman, and Andrew Miller*

**Smart Contracts and Blockchain Identity**

In Code We Trust? Measuring the Control Flow Immutability  
of All Smart Contracts Deployed on Ethereum . . . . . 357  
*Michael Fröwis and Rainer Böhme*

Who Am I? Secure Identity Registration on Distributed Ledgers . . . . . 373  
*Sarah Azouvi, Mustafa Al-Bassam, and Sarah Meiklejohn*

A User-Centric System for Verified Identities on the Bitcoin Blockchain . . . . 390  
*Daniel Augot, Hervé Chabanne, Thomas Chenevier, William George,  
 and Laurent Lambert*

**Short Papers**

Towards a Concurrent and Distributed Route Selection for Payment  
 Channel Networks . . . . . 411  
*Elias Rohrer, Jann-Frederik Laß, and Florian Tschorsch*

Graphene: A New Protocol for Block Propagation Using Set Reconciliation . . . 420  
*A. Pinar Ozisik, Gavin Andresen, George Bissias, Amir Houmansadr,  
 and Brian Levine*

Short Paper: Revisiting Difficulty Control for Blockchain Systems . . . . . 429  
*Dmitry Meshkov, Alexander Chepurnoy, and Marc Jansen*

Secure Event Tickets on a Blockchain . . . . . 437  
*Björn Tackmann*

**Author Index** . . . . . 445